IN THE CLAIMS

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please **AMEND** the claims in accordance with the following:

Please **ADD** new claim 17.

1. (CURRENTLY AMENDED) A cryptographic communication method, comprising:

individually authenticating, in ~~a~~each transmission side, a common communication key and an individual transmission side only key that is different from the common communication key, thereby using both keys to encipher or decode in each transmission side,

determining, in ~~the~~each transmission side, whether a target file is enciphered by the individual transmission side only key,

decoding the target file using the individual transmission side only key, if determined that the target file is enciphered, and not decode processing the target file as an unprocessed target file, if determined that the target file is not enciphered; and

enciphering for transmission, in ~~the~~each transmission side, the decoded target file or the unprocessed target file that is not enciphered, using the common communication key,

wherein in ~~the~~each transmission side, the decoding using the individual transmission side only key and the enciphering using the common communication key are performed continuously, if the decoding is performed.

2. (PREVIOUSLY PRESENTED) The cryptographic communication method according to claim 1, wherein a file identifier of the target file is embedded in a file name of the target file, and a new identifier indicating that the target file is the enciphered target file, is added to the file name of the target file when enciphering the decoded target file or the unprocessed target file by using the communication key.

3. (CURRENTLY AMENDED) A cryptographic communication method, comprising:

individually authenticating, in ~~a~~each reception side, a common communication key and an individual reception side only key that is different from the common communication key, thereby using both keys to encipher or decode in each reception side;

decoding, in ~~the~~each reception side, the received file using the common communication key;

determining, in ~~the~~each reception side, whether a target folder for storing the decoded file is for encipher files,

enciphering the decoded file using the individual reception side only key and storing the enciphered decoded file in the target folder, if the target folder is for encipher files, and storing the decoded file in the target folder without any encipher processing, if the target folder is not for encipher files,

wherein in ~~the~~each reception side the decoding process using the common communication key and the enciphering process using the ~~communication~~individual reception side only key are performed continuously, if the enciphering process is performed.

4. (CANCELLED)

5. (CANCELLED)

6. (CURRENT AMENDED) A cryptographic communication method, comprising:

authenticating, in a transmission side, an individual transmission side only key,

authenticating a common communication key that is different from the individual side only key from among a plurality of common communication keys,

enciphering data to be transmitted in the transmission side using a common communication key from among ~~a~~the plurality of common communication keys,

determining, in the transmission side, whether a target file is enciphered by the individual transmission side only key,

decoding the target file using the individual transmission side only key, if determined that the target file is enciphered, and not decode processing the target file as an unprocessed target file, if determined that the target file is not enciphered,

enciphering for transmission, in the transmission side, the decoded target file or the unprocessed target file that is not enciphered, using the common communication key,

adding an identification code corresponding to the common communication key used for the enciphering, and

decoding, in the reception side, the enciphered target file received, from the transmission side, using a common communication key, from among a plurality of common communication keys, corresponding to the identification code added in the enciphered target file.

7. (CANCELLED)

8. (CANCELLED)

9. (CURRENTLY AMENDED) A file access system, wherein two different keys are authenticated individually, and for data transmission, a decoding process decodes enciphered data stored in an enciphered folder using one of the keys as an individual transmission side only key, and an enciphering process automatically enciphers the decoded data for the transmission using the other of the keys as a common communication key.

10. (CURRENTLY AMENDED) A file access system, wherein two different keys are authenticated individually, and a programmed computer processor controls the file access system according to a process of determining whether a target file to be transmitted is enciphered, decoding the target file by using one of the keys as an individual transmission side only key, if determined that the target file is enciphered, not decode processing the target file as an unprocessed target file, if the target file is not enciphered, and for transmission, enciphering the decoded target file or the unprocessed target file using the other of the keys as a common communication key.

11. (CURRENTLY AMENDED) A file access system, wherein two different keys are authenticated individually, and a programmed computer processor ~~control~~controls the file access system according to a process of decoding an enciphered file received from a transmission side by using one of the keys as a common communication key, determining whether a target folder for storing the decoded file is for encipher files, enciphering the decoded file by using the other of the keys as an individual reception side only key and storing the enciphered decoded file in the target folder, if the target folder is for encipher files, and storing the decoded file in the target

folder without any encipher process, if the target folder is not for encipher files.

12. (CANCELLED)

13. (CURRENTLY AMENDED) A file access system comprising a programmed computer processor controlling the file access system according to a process comprising:

displaying a first folder and a second folder,

decoding and/or enciphering a file stored in the first folder using a first transmission/reception side only key when an instruction is input for moving the file from the first folder to the second folder for transmission of the file,

determining whether the file stored in the first folder is enciphered,

decoding the file by using ~~a~~the first transmission/reception side only key, if determined that the file is enciphered, and not decode processing the file as an unprocessed file, if determined that the file is not enciphered,

enciphering the decoded file or the unprocessed file by using a second common communication key, and

storing the enciphered decoded file or the enciphered unprocessed file in the second folder for the transmission.

14. (CURRENTLY AMENDED) A computer-readable recording medium on which a program of file access is recorded, the program controlling a data transmitting computer according to a process comprising:

individually authenticating a common communication key and an individual transmission side only key that is different from the common communication key, thereby using both keys to encipher or decode in the transmitting computer;

determining whether a target file for transmission is enciphered by the individual transmission side only key;

decoding the target file using the individual transmission side only key, if determined that the target file is enciphered, and not decode processing the target file as an unprocessed target file, if determined that the target file is not enciphered; and

enciphering for transmission the decoded target file or the unprocessed target file that is not enciphered, using the common communication key.

15. (CURRENTLY AMENDED) An encipher processing device that is used for a cryptographic communication, the device comprising:

a common communication key;

an individual transmission side only key that is different from the common communication key;

means for individually authenticating the common communication key and the individual transmission side only key, thereby using both keys to encipher or decode in the encipher processing device;

means for deciding whether a target file is enciphered by the individual transmission side only key;

means for decoding the target file using the individual transmission side only key, if the target file is enciphered;

means for enciphering a decoded target file or a target file that is not enciphered, using the common communication key; and

means for transmitting the target file enciphered by the common communication key;

wherein the decoding process using the transmission side only key and the enciphering process using the common communication key are performed continuously, if the decoding process is performed.

16. (CURRENTLY AMENDED) A cryptographic communication method, comprising:

using a common communication key to a transmission and reception side for enciphering and deciphering data to be transmitted and received by ~~a~~the transmission and reception side, respectively, and

using an individual transmission side only key for decoding enciphered data stored in an enciphered folder at ~~the~~each transmission side and an individual reception side only key for enciphering data to be stored in an enciphered folder at each reception side,

wherein in ~~the~~each transmission side, ~~the individual key is different from the communication key used for enciphering the data to be transmitted~~, first, the stored enciphered data are decoded using the individual transmission side only key ~~first~~, and, second, the decoded data is enciphered using the common communication key for transmission, and

wherein in each reception side, first, the received enciphered data are decoded using the common communication key, and, second, the decoded data is enciphered to be stored in the enciphered folder in the reception side using the individual reception side only key.

17. (NEW) A cryptographic communication method, comprising:

using a common communication key for enciphering a file to be transmitted;

preparing a transmission and reception folder for storing the file to be transmitted by cryptographic communication;

preparing an enciphered folder for automatically performing an enciphering process on a file using an individual transmission/reception side only key to store the file as an enciphered file when the file is moved from another folder to the enciphered folder, and for automatically performing a decoding process on the enciphered file stored in the enciphered folder using the individual transmission/reception side only key when the enciphered file stored in the enciphered folder is moved to another folder;

decoding the file stored in the enciphered folder using the individual transmission/receptions side only key to encipher the decoded file using the common communication key for storing the common communication key enciphered file in the transmission and reception folder, when the file stored in the enciphered folder is moved to the transmission and reception folder;

enciphering the file stored in a folder other than the enciphered folder using the common communication key to store the common communication key enciphered file in the transmission and reception folder, when the file stored in the folder other than the enciphered folder is moved to the transmission and reception folder; and

transmitting the common communication key enciphered file stored in the transmission and reception folder.